UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/838,759	04/19/2001	Lance W. Russell	10003536-1	1330

7590   10/05/2004

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER
KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 10/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/838,759	RUSSELL ET AL.
	Examiner	Art Unit
	Paula W Klimach	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 January 2004</u>.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>08/09/01, 01/05/04</u>.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moore

(6,678,700) in view of Moskowitz (20020071556 A1) and Brundrett et al. (6,249,866).

In reference to claims 1 and 13-14, Moore et al (6,678,700) discloses a method of

receiving at the meta-data server an open-file request that is created by the application

(distributed file interface coupled to the client; column 6 lines 36-45), the open-file request

specifying a name of a first file, wherein the first file includes a first set of blocks (column 6

lines 13-45 in combination with column 18 lines 23-28). The request for the resource would

include the name of the file (Fig. 7 part 40). During the creation of the Meta data creation of

normal objects is used to put data objects into a container at the SRB server (meta data server)

(column 18 lines 37-46), thus creating an object in response to the open-file request. Moore

discloses writing the data to the copy then updating the container. This is the function of

transmitting the object to the file interface because the client and the server have the same copy

of the information on the file interface.

However Moore does not disclose generating an encryption key at the meta-data server

and the storage server.

Moskowitz et al teaches the generation of partial keys at different entities (page 3 paragraph 0023). The first key creator creates the first part of the key as does the meta-data server and the second key creator creates the second part of the key as does the storage server (page 2 paragraph 0015).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use partial keys created at different servers as in the system of Moskowitz and adding the keys to the data portion of the object in the system of Moore, thus creating a security object. One of ordinary skill in the art would have been motivated to do this because sharing the secret between more devices increases the amount of security since both values are required fore decrypting the message.

Moore and Moskowitz do not disclose adding the encrypted block list to the security object.

Brundrett keeps keys in the meta-data (column 4 line 64 to column 5 line 4). The file is encrypted; therefore encrypting a list that identifies the first set of blocks, whereby an encrypted block list is formed (column 15 lines 36-39).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the file as in Brundrett and adding the encrypted information to the data portion of the object in the system of Moore. One of ordinary skill in the art would have been motivated to do this because encryption secures the information.

In reference to claim 2, Moore discloses transmitting a file access request and security object from the distributed file system interface to the storage server in response to a file access

request from a client application (column 6 lines 36-48), the file access request including an operation code and a reference to selected data of a file (column 19 lines 33-39);

Moore and Moskowitz do not disclose decrypting the block list at the storage server in response to the file access request; providing access to the selected data in accordance with the operation code upon successful decryption of the block list.

Brundrett discloses decrypting the text for the NTFS in response from a request from an application and thereby providing access to the selected data upon successful decryption (column 17 lines 6-34).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to decrypt the file as in Brundrett in the system of Moore. One of ordinary skill in the art would have been motivated to do this because decryption makes the encrypted data available to the user.

In reference to claims 3, 8, and 16, Brundrett further discloses encrypting file data at the distributed file interface for file write operations using the encryption key in the security object; and decrypting file data at the distributed file interface for file read operations using the encryption key in the security object (Fig. 17 and Fig. 20).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the file as in Brundrett and adding the encrypted information to the data portion of the object in the system of Moore. One of ordinary skill in the art would have been motivated to do this because encryption secures the information.

In reference to claims 4 and 9, Moore does not disclose a system generating a partial encryption key at the meta-data server and storing the partial encryption key in the security object; transmitting the security object to the storage server; and completing generation of the encryption key at the storage server using the partial encryption key and storing a complete encryption key in the security object; and returning the security object with the complete encryption key to the meta-data server.

Moskowitz discloses a system wherein the key is created at two different devices (page 2 paragraph 0015 and page 3 paragraph 0023).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to create partial keys as in the system of Moskowitz in the system of Moore. One of ordinary skill in the art would have been motivated to do this because security is increased when more than one person possess the key to sensitive information.

In reference to claims 5 and 10, Moore discloses transmitting a close file request, along with the security object, from the distributed file system interface to the meta-data server the close file request specifying the name of the first file; removing the encrypted block list of the first file from the security object (Fig. 10 part 75).

In reference to claims 6 and 11, further comprising returning the security object from the meta-data server to the distributed file system interface after removing the block list. The system of Moore updates the copy of the data in the container; therefore keeping the copy of the client and the server the same as a result the function of sending the object to the server is fulfilled (Fig. 16B).

In reference to claims 7 and 12, Although Moore discloses a close file request Moore, Moskowitz, and Brundrett do not disclose deleting the security object if there are no block lists in the security object after processing a close file request.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to delete the security object if there are no block lists in the security object after a close file request. One of ordinary skill in the art would have been motivated to do this because when the block list is empty there is nothing that is allocated to these blocks and therefore the object takes up space for information that is no longer required.

In reference to claim 15, Moore discloses transmitting a file access request and security object from the distributed file system interface to the storage server in response to a file access request from a client application (column 6 lines 36-48), the file access request including an operation code and a reference to selected data of a file (column 19 lines 33-39). Moore discloses locating the copy of the selected resource (Fig. 16 B part 131), which provides the same result as sending the server the object; the server poses the same copy as the client.

Moore and Moskowitz do not disclose decrypting the block list at the storage server in response to the file access request; providing access to the selected data in accordance with the operation code upon successful decryption of the block list.

Brundrett discloses decrypting the text for the NTFS in response from a request from an application and thereby providing access to the selected data upon successful decryption (column 17 lines 6-34).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to decrypt the file as in Brundrett in the system of Moore. One of ordinary skill in the art would have been motivated to do this because decryption makes the encrypted data available to the user.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.
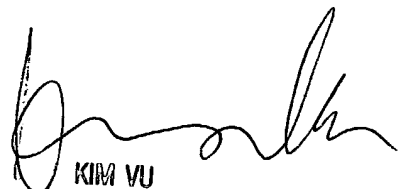
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

The 2100 Tech center will move to Carlyle in October 2004. The new telephone number for the receptionist is (571) 272-2100. The examiner's new telephone number will be (571) 272-3854.

PWK
Tuesday, September 28, 2004

KIM VU
SUPERVISORY PATENT
TECHNOLOGY CE